National Infrastructure Protection Center
CyberNotes

Issue #2003-04 *February 24, 2003*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between February 5 and February 20, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Adalis Informa-tique[1]	Unix	D-Forum 1.0, 1.10, 1.11	A vulnerability exists in the '/includes/header.php3' and '/includes/footer.php3' scripts, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	D-Forum Remote File Include	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.

[1] SecurityFocus, February 18, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Aladdin Know-ledge Systems[2]	Windows 2000	eSafe Gateway 3.0, 3.5	A vulnerability exists because only viruses with the first 15 kb of the content stream are detected when eSafe is used with the Check Point Content Vectoring Protocol (CVP), which could let a remote malicious user send specially crafted malicious content that will bypass security mechanisms.	No workaround or patch available at time of publishing.	eSafe OPSEC CVP Virus Scanning Bypass	Medium	Bug discussed in newsgroups and websites.
Alt-N Technol-ogies[3]	Windows 95/98/NT 4.0/2000	MDaemon 2.8, 2.8.5, 3.0.3, 3.0.4, 3.1.1, 3.1.2, 3.5.0, 3.5.1, 3.5.4, 3.5.6, 5.0.7, 6.0.0, 6.0.5-6.0.7, 6.5.0	A vulnerability exists in the 'Form2Raw.exe' utility, which could let a remote malicious user send forged mail with spoofed headers.	No workaround or patch available at time of publishing.	Alt-N MDaemon/ WorldClient 'Form2Raw' Mail Header Spoofing	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Andries Brouwer[4]	Unix	util-linux 2.11u, 2.11n	A vulnerability exists in the 'mcookie' utility because cookies may be generated in a predictable manner, which could let a malicious user obtain sensitive information.	**Mandrake:** http://www.mandrakesecure.net/en/ftp.php	Util-Linux 'mcookie' Utility	Medium	Bug discussed in newsgroups and websites.
APC[5]	Unix	apcupsd 3.8.5	A vulnerability exists in the 'log_event' function due to a programming error, which could let remote malicious user obtain root access and possibly execute arbitrary code.	Upgrade available at: http://prdownloads.sourceforge.net/apcupsd/apcupsd-3.8.6.tar.gz?download	Apcupsd 'log_event' Remote Root Access	**High**	Bug discussed in newsgroups and websites.
Apple[6]	Unix (OS X)	MacOS X 10.2 (Jaguar), 10.2.1-10.2.3	A vulnerability exists in the TruBlueEnvironment emulator, which could let a malicious user obtain elevated privileges.	Upgrade available at: http://docs.info.apple.com/article.html?artnum=70168	MacOS TruBlue Environment Variable Privilege Escalation CVE Name: CAN-2003-0088	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Apple[7]	Unix (OS X)	MacOS X 10.2 (Jaguar), 10.2.1-10.2.3	A vulnerability exits in 'iDrive' because the File Protocol allows a system administrator to log on as a normal user using administration login details, which could let a malicious user obtain sensitive information.	Upgrade available at: http://docs.info.apple.com/article.html?artnum=70168	Apple File Protocol iDrive Administrator Login CVE Name: CAN-2003-0049	Medium	Bug discussed in newsgroups and websites.

[2] Bugtraq, February 6, 2003.
[3] SecurityTracker Alert ID, 1006058, February 7, 2003.
[4] Mandrake Linux Security Update Advisory, MDKSA-2003:016, February 14, 2003.
[5] SecurityTracker Alert ID, 1006108, February 15, 2003.
[6] @stake, Inc. Security Advisory, February 14, 2003.
[7] Apple Security Update, 61798, February 14, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Aprelium Technol-ogies[8]	Windows, Unix	Abyss Web Server 1.0.7, 1.1.2	A vulnerability exists because failed authentication attempts are not logged and the number of failed authentication attempts to the administrative interface is not limited, which could let a remote malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Abyss Web Server Failed Login Recording	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Bastille[9]	Unix	HP-UX Bastille B.02.00.00	A vulnerability exists in the Bastille Hardening System when used in conjunction with the HP-UX operating system and the Sendmail daemon, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6849AA	HP-UX Bastille sendmail.cf Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Benjamin Low[10]	Windows, Unix	CGI-Lite 2.0	A vulnerability exists in the escape_dangerous_chars() function because specially crafted input can be submitted that will bypass the code's security filtering mechanisms, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	CGI Lite escape_ dangerous_ chars()	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Bharat Mediratta [11]	Unix	Gallery 1.3.3	A vulnerability exists when the 'temp' and 'albums' directories are created and the way image files are managed due to unsafe file permissions, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Gallery Management Software Unsafe File Permissions	Medium	Bug discussed in newsgroups and websites.
BisonFTP [12]	Windows 95/98/NT 4.0	Bison Ftp Server V4R2	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists when a malicious user submits exceptionally long FTP commands such as 'cwd' or 'ls'; and a vulnerability exists when a 'ls' command is issued using the character sequence '@../', which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	BisonFTP Multiple Vulnerabilities	Low/ Medium (Medium if sensitive informa-tion can be obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.
BitchX[13]	Multiple	IRC Client 75p3, 1.0 c20cvs, 1.0 c19, 1.0 c16	A Denial of Service vulnerability exists when a malicious user submits a malformed RPL_NAMREPLY numeric.	No workaround or patch available at time of publishing.	BitchX Malformed RPL_ NAMREPLY Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

[8] Bugtraq, February 12, 2003.
[9] Hewlett-Packard Company Security Bulletin, HPSBUX0203-245, February 13, 2003.
[10] Bugtraq, February 11, 2003.
[11] SecurityTracker Alert ID, 1006066, February 10, 2003.
[12] immune advisory, February 17, 2003.
[13] Bugtraq, February 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Celestial Software[14]	Windows	Absolute Telnet 2.0, 2.11	A buffer overflow vulnerability exists due to insufficient bounds checking when the title bar is set by the client, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.celestialsoftware.net/telnet/beta_software.html	Absolute Telnet Title Bar Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit scripts have been published.
Cheeta Technol-ogies[15]	Windows	CheetaChat 6.5.10	A vulnerability exists because encrypted Yahoo! authentication credentials are stored in a local file, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	CheetaChat Internal Browser Plaintext Password Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited using the CheetaChat client.
Cisco Systems[16]	Multiple	All Cisco IOS if IP routing is disabled.	A vulnerability exists because it is possible to make arbitrary remote modifications to the Cisco IOS routing table if IP routing is disabled, which could let a remote malicious user cause a Denial of Service or intercept communications.	**Workaround:** Cisco reports that you prevent the target router from acting upon received ICMP redirect packets using the following configuration command: Router(config)#no ip icmp redirect	IOS ICMP Redirect Routing Table Modification	Low/ Medium (Medium if communi-cations can be inter-cepted)	Bug discussed in newsgroups and websites. Vulnerability may be exploited with one of several freely available packet crafting tools.
CPanel[17]	Unix	CPanel 5 & prior	Multiple vulnerabilities exist: a vulnerability exists in the 'guestbook.cgi' script, which could let a remote malicious user execute arbitrary commands; and a vulnerability exists in Openwebmail, which could let a malicious user obtain root privileges.	No workaround or patch available at time of publishing.	CPanel 5 'guestbook.cgi' & Openwebmail Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.

[14] Bugtraq, February 6, 2003.
[15] Bugtraq, February 13, 2003.
[16] Cisco Field Notice, 23074, February 10, 2003.
[17] Bugtraq, February 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
DotBr[18]	Unix	BotBr 0.1	Multiple vulnerabilities exist: a vulnerability exists in the 'foo.php3' script due to the way the 'phpinfo()' function is used, which could let a remote malicious user obtain sensitive information; a vulnerability exists because the configuration file doesn't have the proper PHP file extension, which could let a remote malicious user obtain sensitive information; a vulnerability exists in the 'system.php3' script due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary commands; and a vulnerability exists in the 'exec.php3' script due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	DotBr Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Eggheads Develop-ment Team[19]	Unix	Eggdrop IRC bot 1.6.10-1.6.13	A vulnerability exists when linked to a botnet, which could let an unauthorized remote malicious user can use the bot as a proxy.	No workaround or patch available at time of publishing.	Eggdrop IRC Bot Unauthorized Proxy	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited using an IRC client.
Ericsson[20]	Multiple	HM220dp DSL Modem	A vulnerability exists in the remote administration and configuration web interface because no authentication is required, which could let an unauthorized remote malicious user obtain web management interface access.	No workaround or patch available at time of publishing.	HM220dp DSL Modem Administration Interface	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Eset Software[21]	Unix	NOD32 Antivirus 1.0 11, 1.0 12	A buffer overflow vulnerability exists when scanning a directory path of excessive length, which could let a malicious user execute arbitrary commands with superuser privileges.	Upgrade available at: http://www.nod32.com/download/download.htm	NOD32 Antivirus Local Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[18] SecurityFocus, February 15, 2003.
[19] Bugtraq, February 9, 2003.
[20] Bugtraq, February 11, 2003.
[21] iDEFENSE Security Advisory, 02.10.03, February 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Francisco Burzi[22]	Windows, Unix	PHP-Nuke 5.6, 6.0	Several vulnerabilities exist: a vulnerability exists in the 'admin' Cookie Variable used during the authentication process due to insufficient sanitization of cookie based data, which could let a remote malicious user obtain sensitive information; and a vulnerability exists because user-supplied data is insufficiently sanitized when SQL queries are constructed, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PHPNuke 'Admin' Cookie Variable & SQL Query Sanitization	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit has been published for the Search Engine SQL vulnerability.
GNU[23] ***Vendors release patches[24, 25]*** ***RedHat releases patch[26]***	**Unix**	**Fileutils 4.0, 4.1, 4.1.6**	**A race condition vulnerability exists in various utilities, which could let a malicious user delete the whole filesystem.**	**Patch available for 4.1.6 at: http://mail.gnu.org/pipermail/bug-fileutils/2002-March/002440.html** ***Caldera:*** **ftp://ftp.caldera.com/pub/updates/OpenLinux/** ***Mandrake:*** **http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-031.php?dis=8.1** ***RedHat:*** **ftp://updates.redhat.com/6.2/en/os/SRPMS/fileutils-4.0**	**Fileutils Race Condition** **CVE Name: CAN-2002-0435**	**Medium**	**Bug discussed in newsgroups and websites.**
Gupta Technol-ogies[27]	Windows 98/ME/NT 4.0/2000, XP	SQLBase 8.1.0	A buffer overflow vulnerability exists when the 'EXECUTE' command is used, which could let a remote malicious user execute arbitrary code with elevated privileges.	No workaround or patch available at time of publishing.	SQLBase EXECUTE Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Hewlett Packard Company[28]	Unix	HP HP-UX 11.0	A buffer overflow vulnerability exists in the 'disable' utility when strings of excessive length as parsed as the '-r' command line argument, which could let a malicious user cause a memory corruption and possibly execute arbitrary code.	HP has announced that the fixes supplied for a previous lp vulnerability also fix the described issue. Users are advised to apply the necessary fixes supplied in the HPSBUX0208-213 security bulletin.	HP-UX 'disable' Local Buffer Overflow	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[22] Bugtraq, February 20, 2003.
[23] Securiteam, March 15, 2002.
[24] Caldera International, Inc. Security Advisory, CSSA-2002-018.1, May 13, 2002.
[25] Mandrake Linux Security Update Advisory, MDKSA-2002:031, May 16, 2002.
[26] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:015-05, February 12, 2003.
[27] Network Intelligence India Pvt. Ltd. Advisory, February 10, 2003.
[28] Bugtraq, February 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company [29]	Unix	HP-UX 10.0 1, 10.0, 10.1, 10.8-10.10, 10.16, 10.20, 10.24, 10.26, 10.30, 10.34, 11.04, 11.0, 11.11, 11.20, 11.22	A buffer overflow vulnerability exists in the 'landiag' and 'lanadmin' utilities, which could let a malicious user obtain unauthorized access.	**Workaround:** Change the permissions on the affected binaries by issuing the following commands: chmod 555 /usr/sbin/landiag chmod 555 /usr/sbin/lanadmin	HP-UX landiag/ lanadmin Buffer Overflow	Medium	Bug discussed in newsgroups and websites.
Hewlett Packard Company [30]	Unix	HP-UX 10.0 1, 10.0, 10.1, 10.8-10.10, 10.16, 10.20, 10.24, 10.26, 10.30, 10.34, 11.04, 11.0, 11.11, 11.20, 11.22	A buffer overflow vulnerability exists in the 'stmkfont' utility, which could let a malicious user obtain elevated privileges.	Patches available at: http://itrc.hp.com/ Patch PHSS_15423 **Workaround:** For HP-UX 11 systems, it is advised to remove the setuid bit of stmkfont by issuing the following command: chmod 555 /usr/bin/stmkfont	HP-UX 'stmkfont' Buffer Overflow	Medium	Bug discussed in newsgroups and websites.
Hewlett Packard Company [31]	Unix	HP-UX 10.0 1, 10.0, 10.1, 10.8-10.10, 10.16, 10.20, 10.24, 10.26, 10.30, 10.34, 11.04, 11.0, 11.11, 11.20, 11.22	A vulnerability exists in the 'rs.F3000' binary, which could let a malicious user obtain unauthorized access or cause a Denial of Service.	**Workaround:** Remove the execute permissions on the affected binary by issuing the following commands: chmod 444 /usr/lib/X11/Xserver/ucode/screens/hp/rs.F3000	HP-UX rs.F3000 Unauthorized Access	Low/ Medium (Medium if access can be obtained)	Bug discussed in newsgroups and websites.
Hewlett Packard Company [32]	Unix	HP-UX 11.0	A buffer overflow vulnerability exists in the 'rcp' utility due to insufficient bounds checking of command line arguments, which could let a malicious user execute arbitrary code with the privileges of the superuser.	Patch available at: http://hp.cso.uiuc.edu/ftp/pub/hp/mirror/us-support.external.hp.com/s700_800/11.X/PHNE_23003	HP-UX rcp Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[29] Hewlett-Packard Company Security Bulletin, HPSBUX0302-243, February 12, 2003.
[30] Hewlett-Packard Company Security Bulletin, HPSBUX0302-241, February 12, 2003.
[31] Hewlett-Packard Company Security Bulletin, HPSBUX0302-240, February 12, 2003.
[32] SecurityFocus, February 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company [33]	Unix	HP-UX 11.0 4, 11.0, 11.11, 11.20	A buffer overflow vulnerability exists when an excessive amount of data is redirected into wall as a message intended to be broadcast, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	HPUX Wall Message Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Hewlett Packard Company [34]	Unix	HP-UX 10.10, 10.20, 11.0, 11.11, 11.22	A buffer overflow vulnerability exists in the 'rpc.yppasswd' implementation, which could let a malicious user obtain elevated privileges.	HP-UX 10.20 and 11.22 systems are advised to download a replacement rpc.yppasswd binary available at: ftp://yppass:yppass@hprc.external.hp.com/ or ftp://yppass:yppass@192.170.19.51/ Patches available at: http://itrc.hp.com/ Patch PHNE_28102, Patch PHNE_28103	HP-UX 'rpc.yppasswd' Buffer Overflow	Medium	Bug discussed in newsgroups and websites.
Horde[35] ***SuSE releases patch[36]***	**Unix**	**IMP 2.2-2.2.8**	**Multiple SQL injection vulnerabilities exist due to insufficient sanitization of user-supplied input in SQL queries, which could let a remote malicious user corrupt the database.**	**Upgrade available at: http://www.horde.org/imp/3.1/ Debian: http://security.debian.org/pool/updates/main/i/imp/ *SuSE:* ftp://ftp.suse.com/pub/suse**	**Horde IMP Database Files SQL Injection CVE Name: CAN-2003-0025**	**Medium**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**
Hyper mail[37] ***Debian issues upgrade[38]***	**Unix**	**Hypermail 2.1.3, 2.1.4, 2.1.5**	**Several buffer overflow vulnerabilities exist: a buffer overflow vulnerability exists in the parsemail() function, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the 'mail' CGI component when a reverse DNS lookup is performed if the hostname is of excessive length, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the mail CGI program, which could let a remote malicious user send e-mail to arbitrary recipients.**	**Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=18117&release_id=135937 *Debian:* http://security.debian.org/pool/updates/main/h/hypermail/**	**Hypermail Remote Buffer Overflows CVE Name: CAN-2003-0057**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.**

[33] Bugtraq, February 7, 2003.
[34] Hewlett-Packard Company Security Bulletin, HPSBUX0302-242, February 12, 2003.
[35] Debian Security Advisory, DSA 229-2, January 15, 2003.
[36] SuSE Security Announcement, SuSE-SA:2003:0008, February 18, 2003.
[37] Bugtraq, January 27, 2003.
[38] Debian Security Advisory, DSA 248-1, January 31, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM[39]	Unix	AIX 4.3, 5.1, 5.2,	A buffer overflow vulnerability exists in the National Language Support libIM library, which could let a malicious user execute arbitrary code with elevated privileges.	Patches available at: ftp://aix.software.ibm.com/aix/efixes/security/libIM_efix.tar.Z	AIX libIM Buffer Overflow CVE Name: CAN-2003-0087	**High**	Bug discussed in newsgroups and websites.
IBM Lotus[40]	Windows NT 4.0/2000, Unix	Domino 6.0	A buffer overflow vulnerability exists when a HTTP redirect response is performed, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www14.software.ibm.com/webapp/download/search.jsp?q=&cat=&pf=&k=&dt=&go=y&rs=ESD-DMNTSRVRi&S_TACT=&S_CMP=&sb=r	IBM Lotus Domino HTTP Redirect Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
IBM Lotus[41]	Windows NT 4.0/2000, Unix	Domino 6.0	A buffer overflow vulnerability exists in the 's_ViewName/Foldername' options of the PresetFields parameter due to the way client-supplied request parameters are handled, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www14.software.ibm.com/webapp/download/search.jsp?q=&cat=&pf=&k=&dt=&go=y&rs=ESD-DMNTSRVRi&S_TACT=&S_CMP=&sb=r	Lotus Domino Web Server iNotes s_ViewName/ Foldername Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
IBM Lotus[42]	Windows NT 4.0/2000, Unix	Lotus Domino Server 5.0, 6.0	A vulnerability exists due to insufficient sanitization of user requests, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Domino Dot File Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser. Vulnerability has appeared in the press and other public media.
IBM Lotus[43]	Windows NT 4.0/2000, Unix	Lotus Notes Client 6.0	A buffer overflow vulnerability exists in the 'InitializeUsingNotesUser Name' method when an overly long value is submitted, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www14.software.ibm.com/webapp/download/search.jsp?q=&cat=&pf=&k=&dt=&go=y&rs=ESD-NOTECLNTi&S_TACT=&S_CMP=&sb=r	Lotus iNotes ActiveX Control Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[39] IBM Security Advisory, February 12, 2003.
[40] NGSSoftware Insight Security Research Advisory, NISR17022003a, February 17, 2003.
[41] NGSSoftware Insight Security Research Advisory, NISR17022003b, February 17, 2003.
[42] Bugtraq, February 13, 2003.
[43] NGSSoftware Insight Security Research Advisory, NISR17022003c, February 17, 2003

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IndyNews [44]	Unix	IndyNews	Multiple vulnerabilities exist: a vulnerability exists in the delMediaFile() function, which could let an unauthorized malicious user delete media files; a vulnerability exists in the manageMedia() function, which could let an unauthorized malicious user delete or modify various files; and a vulnerability exists in 'alt' tags of a news article due to insufficient sanitization of some HTML tags, which could let a malicious user execute arbitrary code.	Patch available at: http://www.bergamoblog.it/modules.php?name=Downloads&d_op=getit&lid=4	IndyNews delMediaFile() File Deletion	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.
ISC[45] ***Debian releases patch[46]*** ***OpenPKG releases patch[47]***	**Unix**	**DHCPD 3.0.1 1 rc1-rc10**	**A remote Denial of Service vulnerability exists in 'dhcrelay' when a malicious bootp packet is submitted.**	**Debian: http://security.debian.org/pool/updates/main/d/dhcp3/** ***OpenPKG:*** **http://www.openpkg.org/security/OpenPKG-SA-2003.012-dhcpd.html**	**DHCPD dhcrelay Extraneous Network Packets Remote Denial of Service** **CVE Name: CAN-2003-0039**	**Low**	**Bug discussed in newsgroups and websites. Exploit has been published.**
ISOCA[48]	Unix	Cedric Email Reader 0.2, 0.3	Two vulnerabilities exist: a vulnerability exists in the 'email.php' script, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the 'emailreader_execute _on_each_page.inc.php' script, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Cedric Email Reader Remote File Include Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.
Junk buster[49] ***Upgrade now available*** [50]	**Unix**	**Internet Junk buster 2.01**	**A vulnerability exists in the CONNECT method, which could let a remote malicious user make unauthorized connections to arbitrary ports.**	***Upgrade available at:*** **http://internet.junkbuster.com/ijb.html**	**Internet Junkbuster Proxy Unauthorized Connections**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**

[44] Bugtraq, February 14, 2003.
[45] Bugtraq, January 15, 2003.
[46] Debian Security Advisory, DSA 245-1, January 28, 2003.
[47] OpenPKG Security Advisory, OpenPKG-SA-2003.012, February 19, 2003.
[48] Bugtraq, February 9, 2003.
[49] Bugtraq, December 23, 2002.
[50] SecurityFocus, February 11, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
KDE[51, 52] ***More patches released***[53, 54] ***Conectiva releases patches***[55]	**Unix**	**KDE 2.0, 2.0.1, 2.1-2.1.2, 2.2-2.2.2, 3.0-3.0.5**	**Multiple vulnerabilities exist due to a failure to properly quote parameters of instructions passed to a command shell for execution, which could let a local/remote malicious user execute arbitrary commands.**	**Upgrade available at:** **http://download.kde.org/stable/3.0.5a/** ***Debian:*** **http://security.debian.org/pool/updates/main/k/kdeadmin/** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br/**	**KDE Parameter Quoting Shell Command Execution** **CVE Name: CAN-2002-1393**	**High**	**Bug discussed in newsgroups and websites.**
Kietu[56]	Windows, Unix	Kietu 2.0, 2.3	A vulnerability exists because the include path for a configuration file can be specified, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Kietu Hit.PHP Remote File Inclusion	**High**	Bug discussed in newsgroups and websites.
Microsoft [57]	Windows NT 4.0/2000	Windows 2000 Advanced Server, SP1-SP3, Datacenter Server, SP1-SP3, Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, Terminal Services, SP1-SP3, NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Work-station 4.0, SP1-SP6a	A buffer overflow vulnerability exists in the command prompt (cmd.exe) because paths that contain more 256 characters are not handled properly, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Windows cmd.exe CD Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[51] KDE Security Advisory, December 21, 2002.
[52] Gentoo Linux Security Announcement, 200212-9, December 22, 2002.
[53] Gentoo Linux Security Announcement ,200301-11, January 18, 2003.
[54] Debian Security Advisories, DSA 234-1- 238-1, January 22 & 23, 2003.
[55] Conectiva Linux Security Announcement, CLA-2003:569, February 20, 2003.
[56] SecurityFocus, February 15, 2003.
[57] Bugtraq, February 11, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [58]	Windows 95/98/ME/ NT 4.0/2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Profes-sional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3, Windows 95, SR2, Windows 98, SE, ME, Windows NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Work-station 4.0, SP1-SP6a, XP Home, SP1, XP Profes-sional, SP1	A buffer overflow vulnerability exists in 'riched20.dl' when a Rich Text Format (RTF) file is created that contains a large amount of data as an attribute, which could let a malicious user possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Microsoft Riched20.dll Attribute Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[58] Security Defence Stdio vulnerability announcement, 001, February 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [59] *Microsoft updates bulletin [60, 61]*	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0.1, 5.0.1 SP1-SP3, 5.5, 5.5 SP1&2, 6.0, 6.0 SP1	Several vulnerabilities exist: a vulnerability exists because it is possible to bypass the cross-domain security model that Internet Explorer uses when using dialog boxes, which could let a malicious user execute arbitrary code; and a vulnerability exists because it is possible to bypass the cross-domain security model that Internet Explorer implements when using showHelp () functionality, which could let a malicious user execute arbitrary commands. *Bulletin has been updated to include information about the availability of a hot fix that resolves a non-security related issue caused by the IE 6 version of this patch that could affect some users. Under certain conditions, the issue could cause some users to be unable to authenticate to certain Internet web sites such as subscription based sites, or MSN e-mail.*	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-004.asp *Note: Reports indicate that this patch may not install correctly through the WindowsUpdate website. Users are encouraged to download and install the patch manually.* *Note: This hot fix corrects a very specific non-security issue, and the security patch discussed in this Security Bulletin was, and still is, effective in removing the vulnerabilities. More information, including details of how to obtain the hot fix are available at:* http://www.microsoft.com/windows/ie/downloads/critical/813951/default.asp	Internet Explorer Cross-Domain Vulnera-bilities CVE Names: CAN-2003-1326, CAN-2003-1328	High	Bug discussed in newsgroups and websites. *Proof of Concept exploits have been published.*
Mozilla [62] *Conectiva releases patch [63]*	Windows 95/98/ME/ NT 4.0/2000, XP, MacOS 9.0/ 9.0.4/ 9.1/ 9.2/ 9.2.1/9.2.2, MacOS X 10.x, BeOS 5.0, Unix	Mozilla Browser 0.9.3-0.9.9, 1.0, 1.0.1, 1.1; *Galeon Browser 1.2.4-1.2.6*	A vulnerability exists in the implementation of the JavaScript 'onUnload' event handler because requests that the handler launches have the wrong referer, which could let a malicious user obtain sensitive information.	RedHat: ftp://updates.redhat.com/ Mandrake: http://www.mandrakesecure.net/en/ftp.php *Conectiva:* ftp://atualizacoes.conectiva.com.br/	Mozilla OnUnload Referer Information Leakage CVE Name: CAN-2002-1126	Medium	Bug discussed in newsgroups and websites. Proof of Concept has been published. Vulnerability has appeared in the press and other public media.

[59] Microsoft Security Bulletin, MS03-004 V1.1, February 6, 2003.
[60] Microsoft Security Bulletin, MS03-004 V2.0, February 12, 2003.
[61] Microsoft Security Bulletin, MS03-004 V2.1, February 19, 2003.
[62] Securiteam, September 12, 2002.
[63] Conectiva Linux Security Announcement, CLA-2003:568, February 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mozilla[64] *Conectiva releases patch*[65]	Multiple	Mozilla Browser 0.9.7-1.0; *Galeon Browser 1.2.4-1.2.6*	Multiple vulnerabilities exist that have been patched. These vulnerabilities could let a malicious user cause a Denial of Service, obtain sensitive information or cause arbitrary code to be executed. For a complete list of these vulnerabilities, see http://mozilla.org/releases/mozilla1.0.1/security-fixes-1.0.1.html.	Upgrade available at: http://www.mozilla.org/releases/ **RedHat:** ftp://updates.redhat.com/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php *Conectiva*: ftp://atualizacoes.conectiva.com.br/	Mozilla Multiple Vulnera-bilities	Low/ Medium/ High (Low if a Denial of Service, Medium if sensitive informa-tion is obtained and High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
Multiple Vendors[66] *Conectiva releases patch*[67]	Windows 95/98/ME/ NT 4.0/2000, XP, MacOS 9.0/9.0.4/ 9.1/9.2/9.2.1 MacOS X 10.x, Unix, BeOS 5.0	Mozilla Browser 0.9.5-0.9.9, 1.0; Netscape 6.2-6.2.3; Opera Software Opera Web Browser 5.12. 6.0, 6.0.1; *Galeon Browser 1.2.4-1.2.6*	A vulnerability exists when GIF image files are handled that have the width field set to zero, which could let a malicious user cause a Denial of Service or potentially execute arbitrary code.	**Mozilla:** http://www.mozilla.org/releases/ **Netscape:** http://channels.netscape.com/ns/browsers/download.jsp *Conectiva*: ftp://atualizacoes.conectiva.com.br/	Multiple Vendor Zero Width GIF Image Files	Low/High (High if arbitrary code is executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[64] Bugtraq, September 18, 2002.
[65] Conectiva Linux Security Announcement, CLA-2003:568, February 13, 2003.
[66] Securiteam, September 8, 2002.
[67] Conectiva Linux Security Announcement, CLA-2003:568, February 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [68, 69, 70] ***More updates issued*** [71, 72, 73, 74] ***More updates issued*** [75, 76]	**MacOS X 10.2, Unix**	**Apple MacOS X 10.2 (Jaguar), 10.2.2; Easy Software Products CUPS 1.0.4, 1.0.4–8, 1.1.1, 1.1.4-5, 1.1.4-3, 1.1.4-2, 1.1.4, 1.1.6, 1.1.7, 1.1.10, 1.1.12-1.1.15, 1.1.17**	**Several vulnerabilities exist: vulnerability exists in the HTTP server component of the Common UNIX Printing System (CUPS), which could let a local/remote malicious user obtain root privileges; a race condition exists in the creation of /etc/cups/certs/<pid>, which could let a malicious user create or overwrite any file as root; a vulnerability exists because printers can remotely be added to CUPS by sending a specially crafted UDP packet; a remote Denial of Service vulnerability exits due to negative length memcpy() calls; an integer overflow vulnerability exists in the image handling code, which could let a malicious user obtain elevated privileges; a buffer overflow vulnerability exists in the strncat function call in the setup of the 'options' string, which could let a malicious user obtain root access; a vulnerability exists because CUPS improperly checks for zero width images in filters/image-gif.c, which could let a malicious user execute arbitrary code; and a vulnerability exists because the return values of many file and socket operations are not checked, which could let a malicious user cause a Denial of Service.** ***Debian issues update that corrects a library dependency for the libcupsys2 package.***	**Apple:** http://www.info.apple.cpm/kbnum/ **Easy Software:** http://www.cups.org/software.html **SuSE:** ftp://ftp.suse.com/pub/suse ***SCO:*** ftp://ftp.sco.com/pub/updates/OpenLinux/ ***Debian:*** http://security.debian.org/pool/updates/main/c/cupsys/ ***Mandrake:*** http://www.mandrakesecure.net/en/ftp.php ***RedHat:*** ftp://updates.redhat.com ***Debian:*** http://security.debian.org/pool/updates/main/c/cupsys ***Information regarding Apple updates available at:*** http://docs.info.apple.com/article.html?artnum=61798	**CUPS HTTP Multiple Vulnerabilities** **CVE Names: CAN-2002-1366, CAN-2002-1367, CAN-2002-1368, CAN-2002-1369, CAN-2002-1371, CAN-2002-1372, CAN-2002-1383, CAN-2002-1384**	**Low/High** **(High if root access can be obtained or arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Exploits have been published.**

[68] iDEFENSE Security Advisory, December 19, 2002.
[69] Gentoo Linux Security Announcement, 200212-13, December 29, 2002.
[70] SuSE Security Announcement, SuSE-SA:2003:002, January 2, 2003.
[71] SCO Security Advisory, CSSA-2003-004.0, January 21, 2003.
[72] Debian Security Advisory, DSA 232-1, January 20, 2003.
[73] Mandrake Linux Security Update Advisory, MDKSA-2003:001, January 10, 2003.
[74] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:295-07, January 13, 2003.
[75] Debian Security Advisory, DSA 232-2, February 20, 2003.
[76] Apple Security Updates, 61798, February 14, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
myPHP Nuke[77]	Windows, Unix	myPHP Nuke 1.8.8 _final_7, 1.8.8	A Cross-Site Scripting vulnerability exists in the 'links.php' script due to insufficient sanitization of HTML code, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	myPHPNuke Links.php Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.
Netgear[78]	Multiple	FM114P	A Directory Traversal vulnerability exists in the web-configuration interface, which could let an unauthorized remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	FM114P Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Nethack[79]	Unix	Nethack 3.4 .0	A buffer overflow vulnerability exists when a specially crafted command string is submitted to the nethack binary, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Nethack Local Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Open Webmail [80] ***Upgrade now available*** [81]	**Unix**	**Open Webmail 1.70, 1.71**	**A vulnerability exists during the authentication process when an invalid username is entered, which could let a remote malicious user obtain sensitive information.**	***Upgrade available at:*** **http://openwebmail.org/openwebmail/download/**	**Open WebMail Invalid Unsername**	**Medium**	**Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.**
Opera Software[82]	Multiple	Opera Web Browser 6.0.5 win32, 7.0 win32 Beta 1&2	A buffer overflow vulnerability exists when an URL is submitted that contains a specially crafted, long username, which could let a remote malicious user execute arbitrary instructions.	Upgrade available at: http://www.opera.com/download/index.dml?opsys=Windows&lng=en&platform=Windows	Opera Username Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit scripts have been published.
Opera Software[83]	Multiple	Opera Web Browser 6.0.5 win32, 7.0 win32 Beta 1&2, 7.0 win32, 7.01win32	A Denial of Service vulnerability exists in 'opera.PluginContext.'	**Temporary workaround:** Disable Java in the browser configuration.	Opera opera.Plugin Context Native Method Denial Of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[77] Bugtraq, February 20, 2003.
[78] Bugtraq, February 10, 2003.
[79] Bugtraq, February 8, 2003.
[80] Securiteam, November 24, 2002.
[81] SecurityFocus, February 12, 2003.
[82] SecurityFocus, February 10, 2003.
[83] Beauchamp Security:Advisory, February 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Oracle Corporation[84]	Windows NT 4.0/2000, XP, Unix	Oracle 9i Application Server 9.0.2	A vulnerability exists in the 'DAV' functionality due to a format string error in the 'mod_dav' module, which could let a remote malicious user execute arbitrary code.	Workaround and upgrade information available at: http://otn.oracle.com/deploy/security/pdf/2003alert52.pdf	Oracle 9i Application Server DAV_PUBLIC Format String CVE Name: CAN-2002-0842	**High**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the press and other public media.
Oracle Corporation[85]	Windows NT 4.0/2000, XP, Unix	Oracle8 8.0.6, Oracle 8i 8.1.7.1, 8.1.7, Oracle9i 9.0, 9.0.1.3, 9.0.1 .2, 9.0.1, 9.0.2, Oracle9i Release 2 9.2.2, 9.2.1	A buffer overflow vulnerability exists in the 'TO_TIMESTAMP_TZ' function, which could let a malicious user execute arbitrary code.	Oracle has made fixes available. Administrators can download the patches at: http://metalink.oracle.com by entering Bug Number 2642439.	Oracle Database Server TO_TIMESTAMP_TZ Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Oracle Corporation[86]	Windows NT 4.0/2000, XP, Unix	Oracle8 8.0.6, Oracle 8i 8.1.7, Oracle9i 9.0, 9.0.1.3, 9.0.1.2, 9.0.1, 9.0.2, Oracle9i Release 2 9.2.2, 9.2.1	A buffer overflow vulnerability exists in the 'TZ_OFFSET' function, which could let a malicious user execute arbitrary code.	Oracle has made fixes available. Administrators can download the patches at: http://metalink.oracle.com by entering Bug Number 2642267.	Oracle Database Server TZ_OFFSET Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Oracle Corporation[87]	Windows NT 4.0/2000, XP, Unix	Oracle8 8.0.6, Oracle 8i 8.1.7, 8.1.7.1, Oracle9i 9.0, 9.0.1.3, 9.0.1.2, 9.0.1, 9.0.2, Oracle9i Release 2 9.2.2, 9.2.1	A buffer overflow vulnerability exists in the 'ORACLE.EXE' binary due to insufficient bounds checking on external data, which could let a malicious user execute arbitrary code.	Oracle has made fixes available. Administrators can download the patches at: http://metalink.oracle.com by entering Bug Number 2620726.	Oracle Database Server ORACLE.EXE Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[84] Oracle Security Alert #52, February 11, 2003.
[85] Oracle Security Alert #50, February 11, 2003
[86] Oracle Security Alert #49, February 11, 2003
[87] Oracle Security Alert #51, February 11, 2003

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Oracle Corporation[88]	Windows NT 4.0/2000, XP, Unix	Oracle8 8.0.6, Oracle 8i 8.1.7, Oracle9i 9.0, 9.0.1.3, 9.0.1.2, 9.0.1, Oracle9i Release 2 9.2.2, 9.2.1	A buffer overflow vulnerability exists in the 'BFILENAME' function due to insufficient bounds checking on user-supplied input, which could let a malicious user execute arbitrary code.	Oracle has made fixes available. Administrators can download the patches at: http://metalink.oracle.com by entering Bug Number 2642117.	Oracle Database Server DIRECTORY Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
PHP[89] ***RedHat releases patch[90]*** ***More patches released[91, 92, 93]***	**MacOS X 10.x, Unix**	**PHP 4.1.2, 4.2.0-4.2.3**	**A buffer overflow vulnerability exists in the wordwrap() function, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.**	**Upgrade available at: http://www.php.net/downloads.php** ***RedHat:*** **ftp://updates.redhat.com/** ***Engarde:*** **http://ftp.engardelinux.org/pub/engarde/stable/updates/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***SuSE:*** **ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/**	**PHP wordwrap() Buffer Overflow** **CVE Name: CAN-2002-1396**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites.**
PHP Group[94, 95]	Windows, Unix	PHP 4.3	A vulnerability exists in PHP CGI SAPI that makes options for preventing direct access to the CGI binary useless, which could let a malicious user execute arbitrary code.	**OpenPKG:** ftp://ftp.openpkg.org/release/1.2/UPD/ **PGP Group:** http://www.php.net/downloads.php	PHP CGI SAPI Code Execution	**High**	Bug discussed in newsgroups and websites.
phpBB Group[96]	Windows, Unix	phpBB 1.4.0-1.4.4	A vulnerability exists in the 'auth.php' script due to insufficient sanitization of null characters, which could let a malicious user obtain sensitive information and possibly execute arbitrary PHP code.	No workaround or patch available at time of publishing.	PHPBB Auth.PHP File Disclosure	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
phpBB Group[97]	Unix	phpBB 2.0.0-2.0.2	A vulnerability exists due to insufficient sanitization of user-supplied input when a SQL query is constructed, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PHPBB2 Page_Header. PHP SQL Injection	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[88] Oracle Security Alert #51, February 11, 2003
[89] Bugtraq, December 27, 2002.
[90] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:017-06, February 4, 2003.
[91] EnGarde Secure Linux Security Advisory, ESA-20030219-003, February 19, 2003.
[92] Mandrake Linux Security Update Advisory, MDKSA-2003:019, February 20, 2003.
[93] SuSE Security Announcement, SE-SA:2003:0009, February 18, 2003.
[94] PHP Security Advisory, February 17, 2003.
[95] OpenPKG Security Advisory, OpenPKG-SA-2003.010, February 18, 2003.
[96] Bugtraq, February 20, 2003.
[97] Bugtraq, February 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
php-board[98]	Windows, Unix	php-board 1.0	A vulnerability exists because user information is stored in flat files and access is not sufficiently restricted, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PHP-Board User Password Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Posadis Team[99]	Unix	Posadis 0.50.4 - 0.50.8	A remote Denial of Service vulnerability exists due to the way certain DNS queries are read by the server.	Upgrades available at: http://prdownloads.sf.net/posadis/	Posadis DNS Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Postgre SQL[100, 101] ***Mandrake issues upgrade[102]***	**Unix**	**Postgre SQL 6.3.2, 6.5.3, 7.0.3, 7.1-7.1.3, 7.2, 7.2.1**	**A buffer overflow vulnerability exists in the date parser due to insufficient bounds checking, which could let a malicious user cause a Denial of Service or execute arbitrary code.**	**RedHat:** ftp://updates.redhat.com/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/pool/updates/main/p/postgresql **SuSE:** ftp://ftp.suse.com/pub/suse ***Mandrake:*** http://www.mandrakesecure.net/en/ftp.php	**PostgreSQL Date Parser Buffer Overflow** **CVE Name: CAN-2002-1398**	**Low/High (High if arbitrary code is executed)**	**Bug discussed in newsgroups and websites.**
Postgre SQL[103, 104] ***Mandrake issues upgrade[105]***	**Unix**	**Postgre SQL 6.3.2, 6.5.3, 7.0.3, 7.1-7.1.3, 7.2.1**	**Several buffer overflow vulnerabilities exist: a buffer overflow vulnerability exists with the TZ environment variable, which could let a malicious user cause a Denial of Service or execute arbitrary code; and a buffer overflow vulnerability exists with the SET TIME ZONE environment variable, which could let a malicious user cause a Denial of Service or execute arbitrary code.**	**RedHat:** ftp://updates.redhat.com/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/pool/updates/main/p/postgresql **SuSE:** ftp://ftp.suse.com/pub/suse ***Mandrake:*** http://www.mandrakesecure.net/en/ftp.php	**PostgreSQL TZ Environment & SET TIME ZONE Environment Variables Buffer Overflows** **CVE Name: CAN-2002-1402**	**Low/High (High if arbitrary code is executed)**	**Bug discussed in newsgroups and websites.**

[98] SecurityFocus, February 15, 2003.
[99] SecurityTracker Alert, 1006047, February 5, 2003.
[100] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:001-16, January 14, 2003.
[101] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:010-10, January 14, 2003.
[102] Mandrake Linux Security Update Advisory, MDKSA-2002:062-1, February 12, 2003.
[103] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:001-16, January 14, 2003.
[104] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:010-10, January 14, 2003.
[105] Mandrake Linux Security Update Advisory, MDKSA-2002:062-1, February 12, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Postgre SQL[106, 107] *Mandrake issues upgrade*[108]	Unix	Postgre SQL 6.3.2, 6.5.3, 7.0.3, 7.1-7.1.3, 7.2-7.2.3	A buffer overflow vulnerability exists in the 'path_add()' function due to insufficient bounds checking, which could let a malicious user cause a Denial of Service or execute arbitrary code.	**RedHat:** ftp://updates.redhat.com/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/pool/updates/main/p/postgresql ***Mandrake:*** http://www.mandrakesecure.net/en/ftp.php	PostgreSQL path_add() Buffer Overflow	Low/High (High if arbitrary code is executed)	Bug discussed in newsgroups and websites.
Postgre SQL[109, 110] *Mandrake issues upgrade*[111]	Unix	Postgre SQL 6.3.2, 6.5.3, 7.0.3, 7.1-7.1.3, 7.2-7.2.3	Several buffer overflow vulnerabilities exist: a buffer overflow vulnerability exists in the 'path_encode()' function, which could let a remote malicious user execute arbitrary commands; and a buffer overflow vulnerability exits with the 'circle_poly' function, which could let a malicious user cause a Denial of Service or execute arbitrary code.	**RedHat:** ftp://updates.redhat.com/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/pool/updates/main/p/postgresql ***Mandrake:*** http://www.mandrakesecure.net/en/ftp.php	PostgreSQL path_encode() & circle_poly Buffer Overflows CVE Name: CAN-2002-1401	Low/High (High if arbitrary code is executed)	Bug discussed in newsgroups and websites.
Postgre SQL[112] *Mandrake issues upgrade*[113]	Multiple	Postgre SQL 6.3.2, 6.5.3, 7.1, 7.1.1, 7.1.2, 7.2	A buffer overflow vulnerability exists in the in cash_words() function because overly long queries are not handled properly, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.postgresql.org/ **RedHat:** ftp://updates.redhat.com/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/pool/updates/main/p/postgresql **SuSE:** ftp://ftp.suse.com/pub/suse ***Mandrake:*** http://www.mandrakesecure.net/en/ftp.php	PostgreSQL cash_words Buffer Overflow CVE Name: CAN-2002-1397	High	Bug discussed in newsgroups and websites. Exploit has been published.

[106] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:001-16, January 14, 2003.
[107] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:010-10, January 14, 2003.
[108] Mandrake Linux Security Update Advisory, MDKSA-2002:062-1, February 12, 2003.
[109] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:001-16, January 14, 2003.
[110] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:010-10, January 14, 2003.
[111] Mandrake Linux Security Update Advisory, MDKSA-2002:062-1, February 12, 2003.
[112] @(#) Mordred Labs Advisory, 0x0001, August 19, 2002.
[113] Mandrake Linux Security Update Advisory, MDKSA-2002:062-1, February 12, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Postgre SQL[114] ***Mandrake issues upgrade***[115]	**Multiple**	**Postgre SQL 6.3.2, 6.5.3, 7.1, 7.1.1, 7.1.2, 7.2, 7.2.1**	**A buffer overflow vulnerability exists in the repeat() function, which could let a malicious user execute arbitrary code.**	**RedHat:** ftp://updates.redhat.com/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/pool/updates/main/p/postgresql **SuSE:** ftp://ftp.suse.com/pub/suse ***Mandrake:*** http://www.mandrakesecure.net/en/ftp.php	**PostgreSQL Repeat Function Buffer Overflow** **CVE Name: CAN-2002-1400**	**High**	**Bug discussed in newsgroups and websites.**
Postgre SQL[116] ***Mandrake issues upgrade***[117]	**Multiple**	**Postgre SQL 6.3.2, 6.5.3, 7.1, 7.1.1, 7.1.2, 7.2, 7.2.1**	**A buffer overflow vulnerability exists in the lpad() and rpad() functions because overly large integer arguments are handled properly, which could let a malicious user cause a Denial of Service. This vulnerability only affects data bases that were created using special international encodings.**	**RedHat:** ftp://updates.redhat.com/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/pool/updates/main/p/postgresql **SuSE:** ftp://ftp.suse.com/pub/suse ***Mandrake:*** http://www.mandrakesecure.net/en/ftp.php	**PostgreSQL lpad() & rpad() functions Buffer Overflow** **CVE Name: CAN-2002-0972**	**Low**	**Bug discussed in newsgroups and websites.**
RARLAB[118]	Windows NT	FAR 1.65, 1.70 beta 1&4	A buffer overflow vulnerability exists due to insufficient bounds checking when directory paths are parsed, which could let a malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	FAR File Manager Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
RedHat[119] ***Patches now available***[120, 121]	**Unix**	**Linux 7.1, 7.2, 7.3, 8.0**	**A vulnerability exists in the 'pam_xauth' module when running the 'su' utility in conjunction, which could let a malicious user obtain elevated privileges.**	***RedHat:*** ftp://updates.redhat.com ***Mandrake:*** http://www.mandrakesecure.net/en/ftp.php	**PAM pam_xauth Elevated Privileges** **CVE Name: CAN-2002-1160**	**Medium**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**

[114] @(#)Mordred Labs Advisory 0x0003, August 20, 2002.
[115] Mandrake Linux Security Update Advisory, MDKSA-2002:062-1, February 12, 2003.
[116] @(#) Mordred Labs Advisory 0x0004, August 20, 2002.
[117] Mandrake Linux Security Update Advisory, MDKSA-2002:062-1, February 12, 2003.
[118] Securiteam, February 15, 2003.
[119] Bedatec Security Advisory, 200212140001, February 4, 2003.
[120] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:035-10, February 12, 2003.
[121] Mandrake Linux Security Update Advisory, MDKSA-2003:017, February 18, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
RedHat[122]	Unix	Linux 7.2, 7.2 ia64, 7.3, 8.0	A vulnerability exists in the 'useradd' utility due to a failure to set secure permissions for a new user's mail spool directory, which could let a malicious user obtain sensitive information.	Upgrade available at: ftp://updates.redhat.com/	Red Hat useradd Insecure Mail Spool Permissions CVE Name: CAN-2002-1509	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
RedHat[123]	Unix	Linux 8.0 i386	A vulnerability exists because the 'uml_net' utility in kernel-utils packages was incorrectly shipped setuid root, which could let a malicious user obtain elevated privileges.	Upgrade available at: ftp://updates.redhat.com/8.0/en/os/i386/kernel-utils-2.4-8.28.i386.rpm	Red Hat Linux User Mode Linux SetUID Installation CVE Name: CAN-2003-0019	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Research Triangle Software, Inc.[124]	Windows 95/98/ME/ NT/2000, XP	Crypto Buddy 1.0, 1.2	Multiple vulnerabilities exist: a vulnerability exists because the passphrase encryption algorithm generates predictable ciphertext for specific sequences of characters, which could let a malicious user obtain sensitive information; a vulnerability exists because the user-supplied passphrase is not used to encrypt files, which could let a malicious user obtain sensitive information; and a vulnerability exists because passphrases over 55 characters in length are truncated, which could result in a user having a false sense of security.	No workaround or patch available at time of publishing.	CryptoBuddy Multiple Passphrase Encryption Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
Sage[125]	Windows, Unix	Sage 1.0 beta 3	Several vulnerabilities exist: a vulnerability exists in the Content Management System when a request is made for a nonexistent module, which could let a malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists due to insufficient sanitization of input submitted in URI parameters, which could let a malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	Sage Path Disclosure & Cross-Site Scripting	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published. There is no exploit code required for the Cross-Site Scripting vulnerability.

[122] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:057-06, February 18, 2003.
[123] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:056-08, February 7, 2003.
[124] Bugtraq, February 10, 2003.
[125] SecurityFocus, February 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Inc.[126] *Jetty software also affected*[127]	Windows, Unix	Java Web Start 1.0, 1.0.1, 1.0.1_01, 1.0.1_02, 1.2; JRE (Linux Production Release), (Solaris Production Release), (Windows Production Release) 1.3, 1.3_1.3, 1.3_02, 1.3_05, 1.3.1, 1.3.1_01, 1.3.1_03, 1.3.1_05, 1.4, 1.4.1; JSSE 1.0.3; SDK (Linux Production Release), (Solaris Production Release), (Windows Production Release) 1.3_02, 1.3_05, 1.3.1_01, 1.3.1_03, 1.3.1_05, 1.4, 1.4.0_02, 1.4, 1.4.1; *Jetty 4.2.4-4.2.6*	A vulnerability exists because the Java Secure Socket Extension (JSSE), Java Plug-in, and Java Web Start incorrectly validate the digital certificate of a web site, which could let untrustworthy web sites be authenticated for SSL transactions.	Upgrades available at: http://java.sun.com/products/jsse/index-103.html or http://java.sun.com/j2se/ *Jetty upgrade available at:* http://prdownloads.sourceforge.net/jetty/Jetty-4.2.7-src.tgz?download	Sun JSSE/Java Plug-In/Java Web Start Incorrect Certificate Validation	Medium	Bug discussed in newsgroups and websites.

[126] Sun(sm) Alert, 50081, January 23, 2003.
[127] SecurityFocus, February 6, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Inc.[128]	Unix	Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0	A remote Denial of Service vulnerability exists when processing malicious packets sent to a listening RPC service.	Patches available at: http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=105402&rev=41 Patch 105402-41, Patch 105401-41, Patch 106943-24, Patch 106942-24, Patch 108828-37, Patch 108827-36, Patch 113319-04	Sun Solaris Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[129]	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86	A vulnerability exists in the mail program due to a problem with the handling of opening mail spool files, which could let a malicious user obtain sensitive information.	Patches available at: http://sunsolve.sun.com Patch 109267-05, Patch 109266-05, Patch 109254-07, Patch 109253-07, Patch 111875-06, Patch 111874-06, Patch 114134-01, Patch 114133-01	Solaris Mail Reading Local Race Condition	Medium	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[130] ***Sun updates bulletin[131]***	**Unix**	**Solaris 2.6, 7, 8, 9**	**A remote Denial of Service vulnerability exists in the 'in.ftpd' daemon.** ***Temporary patches available and updated relief/workaround section.***	**Workaround: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50240**	**Solaris Remote Denial of Service**	**Low**	**Bug discussed in newsgroups and websites.**
Symantec[132]	Windows 98/ME/NT 4.0/2000, XP	Norton AntiVirus 2002	A buffer overflow vulnerability exists when an e-mail message with a compressed file that includes a file with an unusually long filename is received, which could let a malicious user execute arbitrary code.	Product updates containing the fix have been distributed via LiveUpdate.	Norton Antivirus 2002 Email Scanner Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[128] Sun(sm) Alert Notification, 50626, February 18, 2003.
[129] Sun(sm) Alert Notification, 50751, February 11, 2003.
[130] Sun(sm) Alert, 50240, January 27, 2003.
[131] Sun(sm) Alert, 50240, February 6, 2003.
[132] SNS Advisory No.61, February 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
University of Kansas[133] ***More patches released***[134, 135]	**Multiple**	**Lynx 2.8.2 rel.1- 2.8.4 rel.1, 2.8.5 dev.8**	**A vulnerability exists when carriage return and line feed (CRLF) characters are included in the commandline, which could let a malicious user make scripts that use Lynx for downloading files from the wrong site on a web server with multiple virtual hosts.**	**Patch available at:** ftp://lynx.isc.org/lynx2.8.4/patches/lynx2.8.4rel.1c.patch **ELinks:** http://elinks.or.cz/download/elinks-0.4pre15.tar.bz2 **Debian:** http://security.debian.org/pool/updates/main/l/lynx-ssl/ **SCO:** ftp://ftp.sco.com/pub/updates/OpenLinux/ **Trustix:** ftp://ftp.trustix.net/pub/Trustix/updates/ ***RedHat:*** ftp://updates.redhat.com/ ***OpenPKG:*** http://www.openpkg.org/security/OpenPKG-SA-2003.011-lynx.html	**Lynx Command Line URL CRLF Injection**	**Medium**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
Visual Mining, Inc.[136]	Windows NT 4.0/ 2000, XP, Unix	Netcharts XBRL Server 4.0	A vulnerability exists because invalid chunked encoded HTTP requests are insufficiently handled, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Netcharts Server Chunked Encoding Information Leakage	Medium	Bug discussed in newsgroups and websites.
W3M[137, 138, 139, 140, 141]	Windows, Unix	W3M 0.2-0.2.5.1, 0.3--0.3.2; w3mmee 0.3.p23.3, w3mmee-ssl 0.3.p23.3	Two Cross-Site Scripting vulnerabilities exist: a vulnerability exists if frames support is enabled due to insufficient sanitization of HTML tags, which could let a remote malicious user execute arbitrary code; and a vulnerability exists due to inadequate sanitization of IMAGE tags, which could let a remote malicious user execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/w/w3mmee **RedHat:** ftp://updates.redhat.com/ **W3M:** http://prdownloads.sourceforge.net/w3m/w3m-0.3.2.2.tar.gz?download **OpenPKG:** http://www.openpkg.org/security/OpenPKG-SA-2003.009-w3m.html	W3M Cross-Site Scripting CVE Names: CAN-2002-1335, CAN-2002-1348	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

[133] Bugtraq, August 19, 2002.
[134] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:029-06, February 12, 2003.
[135] OpenPKG Security Advisory, OpenPKG-SA-2003.011, February 18, 2003.
[136] Securiteam, February 17, 2003.
[137] Debian Security Advisory, DSA 249-1, February 11, 2003.
[138] Debian Security Advisory, DSA 250-1, February 12, 2003.
[139] Debian Security Advisory, DSA 251-1, February 14, 2003.
[140] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:044-20, February 7, 2003.
[141] OpenPKG Security Advisory, OpenPKG-SA-2003.009, February 18, 2003.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between February 10 and February 21, 2003, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 17 scripts, programs, and net-news messages containing holes or exploits were identified. Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
February 21, 2003	Tcpscan3.txt	Coding a TCP Connect Port Scanner Using VLSM Handbook is an in-depth beginner's tutorial written to explain incorporation of VLSM and CIDR capabilities into a network scanner.
February 20, 2003	**DSR-cpanel.c**	**Script that exploits the CPanel 5 'gueltbook.cgi' vulnerability.**
February 20, 2003	**DSR-nethack.c**	**Script that exploits the Nethack Local Buffer Overflow vulnerability.**
February 20, 2003	PHPBBAutoSelectFishAttacker.php	Exploit for the PHPBB2 Page_Header.PHP SQL Injection vulnerability.
February 20, 2003	**PHPNukeAutoSelectFishAttacker.php**	**Exploit for the PHPNuke Search Engine SQL Injection vulnerability.**
February 20, 2003	**Webmail_local.pl**	**Script that exploits the CPanel 5 Openwebmail vulnerability.**
February 19, 2003	Gobbler-1.8alpha.tar.gz	A tool that is designed to audit various aspects of DHCP networks, from detecting if DHCP is running on a network to performing a denial of service attack. Gobbler also exploits DHCP and Ethernet, to allow distributed spoofed port scanning with the added bonus of being able to sniff the reply from a spoofed host.
February 18, 2003	Absolute_uk2.pl	Perl script that exploits the Absolute Telnet Title Bar Buffer Overflow vulnerability.
February 18, 2003	Xperl_yabbse_mass.tar.gz	Yabase v1.5.0 and below remote scanner / exploit tool which takes advantage of a bug in an include named Packages.php.
February 16, 2003	**Bitchx-353.c**	**Script that exploits the BitchX Malformed RPL_ NAMREPLY Denial of Service vulnerability.**
February 13, 2003	Udp-remote-final.tar.gz	A utility that demonstrates a simple UDP backdoor which allows for remote program execution on a Unix server.
February 11, 2003	Smtpscan-0.4.tar.gz	A tool to guess which MTA is used by sending several "special" SMTP requests and by comparing error codes returned with those in the fingerprint database.
February 10, 2003	030217_o6unexp.tgz	Script that exploits the Opera Username Remote Buffer Overflow vulnerability.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
February 10, 2003	**Nethack.pl**	**Perl script that exploits the Nethack Local Buffer Overflow vulnerability.**
February 10, 2003	**Nethacker.c**	**Script that exploits the BitchX Malformed RPL_ NAMREPLY Denial of Service vulnerability.**
February 10, 2003	o6unexp.c	Script that exploits the Opera Username Remote Buffer Overflow vulnerability.
February 10, 2003	THCunREAL.zip	Remote root exploit for Realserver 8 on several Windows platforms.

Trends

- **Systems are being compromised through the exploitation of null or weak default 'sa' passwords in Microsoft SQL Server and Microsoft Data Engine.**
- **Propagation of SQL 'Slammer' or 'Sapphire' malicious code is still causing varied levels of network degradation across the Internet and the compromise of vulnerable machines.**
- **NIPC has issued an advisory regarding the propagation of an SQL worm. The self-propagating malicious code exploits multiple vulnerabilities in the Resolution Service of Microsoft SQL Server 2000. This worm activity appears to have caused various levels of network degradation across the Internet. In addition to the compromise of vulnerable machines; the apparent effects of this fast-spreading, virus-like infection has overwhelmed the world's digital pipelines and interfered with Web browsing and delivery of e-mail. For more information, see Virus Section, WORM_SQLP1434.A description and NIPC Advisory 03-001.1, located at: http://www.nipc.gov/warnings/advisories/2003/03-001.1updates.htm. For patch information, see:**
  - **http://www.microsoft.com/security/slammer.asp**
  - **http://www.microsoft.com/technet/security/bulletin/MS02-061.asp**
  - **http://www.microsoft.com/technet/security/bulletin/MS02-039.asp**
- **The CERT/CC has released an advisory regarding a buffer overflow vulnerability in the Microsoft Windows Shell. For more information, see Bugs, Holes & Patches table entry, "Windows XP WMA/MP3 Buffer Overflow" and CERT® Advisory CA-2002-37, located at: http://www.cert.org/advisories/CA-2002-37.html.**
- **The CERT/CC has released an advisory regarding multiple vendors' implementations of the secure shell (SSH) transport layer protocol contain vulnerabilities that could allow a remote malicious user to execute arbitrary code with the privileges of the SSH process or cause a denial of service. The vulnerabilities affect SSH clients and servers, and they occur before user authentication takes place. For more information, see Bugs, Holes & Patches table entry "Multiple Vendor SSH2 Implementation" and CERT® Advisory CA-2002-36, located at: http://www.cert.org/advisories/CA-2002-36.html.**
- **The CERT/CC has received reports of increased scanning for NetBIOS services. Probes to port 137/udp may be indicative of such activity.**

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

BAT.Junkboat.Worm (Alias: I-Worm.Junkboat) (Batch File Worm): This is a worm that uses the KaZaA-file sharing network and mIRC to spread. It also creates the file C:\Love_Me.vbs that has the ability to e-mail the BAT.Junkboat.Worm to all addresses in the Microsoft Outlook Address Book.

VBS.Caser@mm (Alias: VBS.Casechange.A) (Visual Basic Script Worm): This is a mass-mailing worm that spreads using Microsoft Outlook and IRC and copies itself across mapped drives. The worm attempts to overwrite several files on your system. The e-mail will have an attachment with a .vbs file extension.

VBS/Cian-C (Aliases: I-Worm.Thery.b, VBS_CIAN.C, VBS.Cian.C@mm, VBS.Cian.C) (Visual Basic Script Worm): This is a worm which spreads via mIRC, P2P file sharing networks, and e-mail attachments. It appends itself to files with the extensions VBS or VBE and infects Word and Excel documents. Infected Word and Excel documents are detected as OF97/Cian-C. Upon execution, VBS/Cian-C drops several copies of itself to the system folder as Winstart.vbs, Wininst32.vbs, Winnt32.vbs, and Winnet32.vbs. The worm also drops itself to the Windows folder as Netlnk32.vbs and Conversation.vbe. VBS/Cian-C then sets the following registry entry in order to run itself on startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Winstart ="Wscript.exe C:\<Systems>\Winstart.vbs %1"

It drops two macro scripts, evade.jpg and evade.gif, to the system folder. The worm then uses these scripts to create the infected Excel Document Personal.xls in the Excel startup folder and infects the Word Document template. Personal.xls and the infected Word Document template will infect Excel and Word documents under the Microsoft Office environment. The infected Office documents can spread separately as viruses and via e-mail, however they will also drop and run a copy of VBS/Cian-C. It lowers the security settings under Microsoft Office by modifying the following registry entries:

- HKCU\Software\Microsoft\Office\<Version>\Excel\Security\AccessVBOM="1"
- HKCU\Software\Microsoft\Office\<Version>\Excel\Security\Level="1"
- HKCU\Software\Microsoft\Office\<Version>\Word\Security\AccessVBOM="1"
- HKCU\Software\Microsoft\Office\<Version>\Word\Security\Level="1"

VBS/Cian-C then proceeds to append itself to files with the extensions VBS and VBE found in various folders. In addition, VBS/Cian-C targets the numerous folders that are the file sharing folders of various Peer-to-peer file sharing applications. VBS/Cian-C replaces files with the following extensions with copies of itself, preserving the filename but adding an additional VBS extension (e.g. filename.mp3.vbs). It then attempts to modify script.ini in the mIRC folder so that the mIRC client will automatically send a copy of the worm to users joining the same IRC channel. The message sent is "Remember this funny conversion I had on IRC?" and the file is Conversation.vbe, detected as mIRC/Cian-C. Finally, VBS/Cian-C sets the following registry entry as infection mark:

- HKCU\Sofware\Zed/[rRlf]\VBS/Evade\ = "VBS/Evade.A by Zed/[rRlf]"

VBS.DLetter@mm (Aliases: VBS/DeathLetter, VBS/Grimgram@MM) (Visual Basic Script Worm): When executed, the worm attempts to send itself to all the recipients in the Microsoft Outlook address book. The e-mail will have a subject that is randomly chosen from a predetermined list and an attachment with a .mht file extension. VBS.DLetter@mm also spreads using the IRC, mIRC, and KaZaA-shared folders.

VBS.Gpremier@mm (Visual Basic Script Worm): This is a mass-mailing worm that is written in the Visual Basic Scripting (VBS) language. When it is executed, it copies itself to the \Windows\System folder and infects all the HTML files with the VBS.CandyLove virus. VBS.Gpremier@mm mails itself to all the contacts in all the Microsoft Outlook Address Books. The e-mail would have the following characteristics:

- Subject: NO estimado Bill G.
- Attachment: gpremier.vbs

VBS.MrCopy.Worm (Visual Basic Script Worm): This worm spreads by copying itself over all the existing .vbs and .vbe files found on all the local drives and mapped network drives. When MrCopy.Worm is activated, it adds the value, "WinUpdate" = "Wscript.exe %System%\Mr. Worm.pps.vbs %," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Next it copies itself as %System%\Mr. Worm.pps.vbs and copies over all the .vbs and .vbe files found on all the local drives and mapped network drives.

W32/Axam-A (Aliases: I-Worm.Axam, W95/MaxaP2P.A, W32.HLLW.Maax@mm, W32/Maax@MM, W32/MaxaP2P.A) (Win32 Worm): This is an e-mail and peer-to-peer worm. The worm may also be found in the numerous folders commonly shared by popular peer-to-peer networking software. It will also be copied to the Windows startup folder and C:\Windows\Application Data\. The following registry entry will be created to run the worm when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\sysaxam32

A new file type named spitmaxa will be created via the registry entry HKCR\Spitmaxa and the registry entry HKCR\.exe will be modified so that EXE files will be run as the file type spitmaxa. This will cause the worm to be run whenever the infected user attempts to run an EXE file. When run, W32/Axam-A will display a message box. On the second of the month a message box will be displayed containing the text "Apa yang membuatkan seseorang itu lalai? Jawapannya ada pada anda sendiri. Dengarlah nasihat dari Axam Virus ini." The virus author Melhacker claims to be based in Malaysia and the text displayed in the message box above is written in the Malay language. Translated it reads "What makes a person careless? The answer is in yourself. Listen to the advice of the Axam Virus." The file Autoexec.bat will be modified to display "...-= AxAm WOrm PreSenT =-..." when executed. W32/Axam-A contains functionality that is intended to delete a large number of files and format drives C: and D:, but this will never work.

W32.Blitzdung@mm (Aliases: I-Worm.Blitzdung, WORM_BLITZDUN.A) (Win32 Worm): This is a mass-mailing worm that was originally written in Java. A converter tool was used to convert the worm to a Win32 Portable Executable (PE) file. It attempts to send a copy of itself to all the contacts found in the Yahoo! Messenger log file. It can also spread through any mIRC channels that you visit. The worm tries to copy a file infected with W32.ElKern.4926 into the Windows folder.

W32.HLLW.Discoball (Alias: W32/Discoball.Worm) (Win32 Worm): This is a worm that spreads through network shares. The existence of the file Mdbole.exe, Seg32.exe or Wins.exe is a sign of a possible infection.

W32.HLLW.Oror.D@mm (Aliases: I-Worm.Roron.4999.c, W32/Roro.V@mm, W32/Roron.AA@mm) (Win32 Worm): This is a mass-mailing worm and a variant of W32.HLLW.Oror@mm. This worm attempts to spread through e-mail, mIRC, KaZaA, network shares, and mapped drives. It also attempts to terminate and remove various security products from the infected computer. This threat is written in the C++ language and is compressed with UPX. The uncompressed size is about 160 KB.

W32.Kwbot.C.Worm (Win32 Worm): This worm attempts to spread itself through the KaZaA and iMesh file-sharing networks. The worm also has a backdoor Trojan capability that allows a malicious user to gain control of the compromised computer.

W32.Kwbot.D.Worm (Win32 Worm): This is a variant of W32.Kwbot.C.Worm, with the following differences:

- This variant was packed using a run-time compression utility.
- The file name has been changed to Winsys.exe.
- The registry entry is named Winsys.

Everything else, including the functionality, remains the same as the W32.Kwbot.C.Worm.

W32/Proget.worm.b (Aliases: W32.Proge, W32/Proget-B, Win32.HLLW.Proget.b) (Win32 Worm): This is a floppy worm virus that creates thousands of 10 byte files on the local system. When run, the worm copies itself to the WINDOWS SYSTEM (%SysDir%) directory, keeping the same filename as when it was run. It creates a registry run key to load itself at startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ Run "%FileName%" = %WormPath%

Once installation is complete, the worm exists. Upon reload, the worm is run from the SYSTEM directory, which activates its propagation routine and payload. The virus has a payload to create a 10 byte file in each directory on the local system using a random 8 character followed by the extension aaa. The content of the file also contains 10 random characters. This action happens each time the system is rebooted, which can result in thousands of files getting created, filling up the hard disk over time. Each minute, a copy of the worm is saved to the A:\ drive.

W32.Yalat.Worm (Aliases: I-Worm.Haelp, W32/Yalat.worm) (Win32 Worm): This is a worm that attempts to spread by using MAPI and by copying itself to shared folders. It also attempts to stop the processes of some antivirus programs. Due to bugs in the code, the worm does not work as intended.

W32.Zokrim@mm (Win32 Worm): This is a mass-mailing worm that uses Microsoft Outlook to send itself to all the contacts in the Outlook Address Book. The worm displays a message when run. The e-mail has the following characteristics:

- Subject: SMS for YOU by Valentina
- Message: Mirko (z) is crazy for Valentina...!!!!!!
- Attachment: Vale.exe

W32.Zokrim@mm is written in the Microsoft Visual Basic programming language.

W97M.Babals.B (Aliases: Word97.Babals, W97M/Bablas.DY) (Word 97 Macro Virus): When W97M.Babals.B is executed, it attempts to infect the Microsoft Word Normal.dot template. Once that happens, the virus will infect any documents that you open or close.

W97M.Cian.C@mm (Word 97 Macro Virus): This is a mass-mailing macro virus that infects Microsoft Word documents. This macro virus has a VBS script inside itself that it inserts and executes on the system.

W97M.Hopel.A (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents when you click Open, Close, Save, New, or Exit. This virus has many different payloads that it can execute on Exit. If an infected document is double-clicked, the virus saves the infected document as C:\Windows\Command\Nt.txt. W97M.Hopel.A also overwrites the Autoexec.bat file with a non-ASCII character.

W97M.Tang (Word 97 Macro Virus): This is the macro module of W32.HLLW.Tang@mm. It infects Microsoft Word documents and templates.

W97M.Tolu (Word 97 Macro Virus): This is a Microsoft Word 97 macro virus that infects Microsoft Word documents and templates. The virus displays an illustration with a message when an infected document is opened.

W97M.Trug.A (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents when they are opened or closed. W97M.Trug.A attempts to hide its malicious actions and it may delete several files from the system.

WORM_LOVEGATE.B (Alias: LOVGATE.A, W32/Lovgate.worm, WORM_LOVGATE.A, I-Worm.Supnot) (Internet Worm): This malware is both a worm and backdoor program. To propagate, it drops copies of itself in network shared folders and subfolders. As a backdoor, it opens a port, 10168 by default, allowing remote malicious users to access and manipulate the affected system. It sends a notification to either of the following e-mail addresses:

- 54love@fescomail.net
- hacker117@163.com

Worm/SMachine.IRC (IRC Worm): This is an Internet worm that spreads through the use of the mIRC network. If executed, the worm creates numerous new files. Additionally, so that it gets run each time a user restart their computer the following file gets modified:

- C:\Windows\Win.ini
  load=
  load=C:\Windows\Inf\Inf\System.exe, C:\Windows\Inf\Inf\System.exe

The following registry keys will also get added:

- HKEY_CLASSES_ROOT\CLSID\{D5DE8D20-5BB8-11D1-A1E3-0A0C90F2731}\InProcServer32
  @="C:\\WINDOWS\\INF\\INF\\MSVBVM60.DLL"
  "ThreadingModel"="Apartment"
- HKEY_CLASSES_ROOT\TypeLib\{000204EF-0000-0000-C000-000000000046}\6.0\9\win32
  @="C:\\WINDOWS\\INF\\INF\\MSVBVM60.DLL"
- HKEY_LOCAL_MACHINE\Software\CLASSES\irc\Shell\open\command
  @="\"C:\\WINDOWS\\INF\\INF\\MIRC.EXE\" -noconnect"

WORM_TANG.A (Aliases: Win32/Gant.A@mm, I-Worm.Tanger, W32.HLLW.Tang@mm, W32/Gant@MM) (Internet Worm): This memory-resident worm propagates in various ways. It sends itself via e-mail to all addresses listed in the Microsoft Outlook address book, via Internet Relay Chat (IRC), mapped network drives, and via popular peer-to-peer file-sharing applications such as KaZaA, Morpheus, Grokster, and others. Aside from carrying out various propagation routines, the worm also infects batch files. Its code also indicates that it has capabilities to infect Word and Excel documents. This malware is developed in Visual Basic and runs on Windows 95, 98, NT, 2000, ME and XP systems. It usually arrives UPX-compressed.

X97M.Cian.C@mm (Excel 97 Macro Virus): This is a mass-mailing macro virus that infects Microsoft Excel spreadsheets. This macro virus has a VBS script inside itself that it inserts and executes on the system.

X97M.Tang (Excel 97 Macro Virus): This is the macro module of W32.HLLW.Tang@mm. It infects Microsoft Excel Spreadsheets.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
AdwareDropper-A	**A**	**Current Issue**
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	**E**	**Current Issue**
Backdoor.Beasty	N/A	CyberNotes-2003-02
Backdoor.Beasty.B	B	CyberNotes-2003-03
Backdoor.Bmbot	**N/A**	**Current Issue**
Backdoor.CHCP	N/A	CyberNotes-2003-03

Trojan	Version	CyberNotes Issue #
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Cow	N/A	CyberNotes-2003-01
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Dani	**N/A**	**Current Issue**
Backdoor.Deftcode	N/A	CyberNotes-2003-01
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.FTP.Casus	N/A	CyberNotes-2003-02
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	**N/A**	**Current Issue**
Backdoor.Hitcap	**N/A**	**Current Issue**
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Cloner	**N/A**	**Current Issue**
Backdoor.IRC.Zcrew	**N/A**	**Current Issue**
Backdoor.Khaos	**N/A**	**Current Issue**
Backdoor.Kilo	**N/A**	**Current Issue**
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.Massaker	N/A	CyberNotes-2003-02
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01
Backdoor.OICQSer.17	17	CyberNotes-2003-01
Backdoor.Optix.04.d	**04.d**	**Current Issue**
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.Remohak.16	16	CyberNotes-2003-01
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.SchoolBus.B	**B**	**Current Issue**
Backdoor.Sdbot.C	C	CyberNotes-2003-02
Backdoor.Sdbot.D	D	CyberNotes-2003-03
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.SilverFTP	**N/A**	**Current Issue**
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Snowdoor	**N/A**	**Current Issue**
Backdoor.Talex	N/A	CyberNotes-2003-02
Backdoor.Udps.10	10	CyberNotes-2003-03
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Xeory	N/A	CyberNotes-2003-03
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zix	N/A	CyberNotes-2003-02
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AOK	N/A	CyberNotes-2003-01
BDS/AntiPC	N/A	CyberNotes-2003-02

Trojan	Version	CyberNotes Issue #
BDS/Backstab	N/A	CyberNotes-2003-02
BDS/Evolut	N/A	CyberNotes-2003-03
DoS-iFrameNet	**N/A**	**Current Issue**
Downloader-BO.dr.b	N/A	CyberNotes-2003-02
Downloader-BS	N/A	CyberNotes-2003-02
Exploit-IISInjector	N/A	CyberNotes-2003-03
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03
IRC/Flood.bi	N/A	CyberNotes-2003-03
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
JS.Seeker.J	J	CyberNotes-2003-01
JS/Seeker-C	**C**	**Current Issue**
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
MultiDropper-FD	N/A	CyberNotes-2003-01
Pac	**N/A**	**Current Issue**
ProcKill-Z	N/A	CyberNotes-2003-03
PWS-Aileen	**N/A**	**Current Issue**
PWSteal.AlLight	N/A	CyberNotes-2003-01
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWS-Tenbot	N/A	CyberNotes-2003-01
QDel359	N/A	CyberNotes-2003-01
Renamer.c	N/A	CyberNotes-2003-03
Tellafriend.Trojan	**N/A**	**Current Issue**
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
Tr/SpBit.A	**A**	**Current Issue**
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Dloader-BO	N/A	CyberNotes-2003-02
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/TKBot-A	**A**	**Current Issue**
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Dasmin.B	B	CyberNotes-2003-03
Trojan.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Idly	**N/A**	**Current Issue**
Trojan.Ivanet	N/A	CyberNotes-2003-02
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.ProteBoy	**N/A**	**Current Issue**
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.Qforager	N/A	CyberNotes-2003-02

Trojan	Version	CyberNotes Issue #
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
VBS.Moon.B	B	CyberNotes-2003-02
VBS.StartPage	N/A	CyberNotes-2003-02
W32.Benpao.Trojan	**N/A**	**Current Issue**
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Systentry.Trojan	N/A	CyberNotes-2003-03
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	**N/A**	**Current Issue**
W32/Igloo-15	**N/A**	**Current Issue**
Xin	N/A	CyberNotes-2003-03

AdwareDropper-A: This is an Adware dropping Trojan. When run, it installs a Macromedia Flash "card," and three Adware DLL files that are Internet Explorer Browser Helper Objects, designed to display advertisements, track the URLs visited on the system, capture typed search strings, and alter the browser's default start page. These DLL files are not considered to be malicious, but are likely used for marketing purposes. As the main installer executable does not contain any end user license agreement (EULA), it is considered malicious. The following message is believed to have been SPAMED to a number of users.

- From: cupid@valentines-ecard.com

The message links to an executable file named card.exe. When run, a Flash "card" is displayed. The executable extracts several files to disk:

- %Program Files%\Valintines Day Card\Valintines Day Card\uninstall.exe
- %Program Files%\Valintines Day Card\Valintines Day Card\valsday.exe
- %Start Menu\Programs%\Valintines Day Card\Uninstall.lnk
- %Start Menu\Programs%\Valintines Day Card\Valintines Day Card.lnk
- %SysDir%\HmePge.dll
- %SysDir%\HotLink.dll
- %SysDir%\IEBrw.dll

Backdoor.Assasin.E: This Trojan is a variant of Backdoor.Assasin. It gives a malicious user unauthorized access to the compromised computer and attempts to terminate the active processes of various firewalls, as well as antivirus and security products. This variant also attempts to spread itself across the network shares. Backdoor.Assasin.E is written in the Borland Delphi programming language and is compressed with UPX.

Backdoor.Bmbot (Alias: W32/Cult.Worm): This is a backdoor Trojan that allows a malicious user to gain control of your computer by using Internet Relay Chat (IRC). A false error message is displayed if Backdoor.Bmbot is not executed from the %System% folder.

Backdoor.Dani (Alias: Backdoor.Dani.20): This is a backdoor Trojan that is written in the Microsoft Visual Basic programming language. It overwrites the Windows registry editor program located in %Windir%\Regedit.exe with a copy of itself. The Trojan allows unauthorized access to an infected computer.

Backdoor.Hipo: This is a typical Backdoor Trojan that allows a malicious user to gain access to and remotely control an infected computer. The Trojan is written in the Delphi programming language and is compressed with UPX.

Backdoor.Hitcap: This is a Backdoor Trojan that gives a malicious user unauthorized access to your computer. It consists of two components:

- An executable file: The executable file is packed with ASPack v1.06.
- A .dll file: The .dll file is packed with PECompact v1.50.

Backdoor.IRC.Cloner (Aliases: Backdoor.IRC.Cloner, BKDR_IRCCLONER, IRC_CLONER, Backdoor:IRC/Cloner): This is a backdoor Trojan that uses mIRC to communicate with a remote malicious user. It allows the malicious user to gain full control over your computer.

Backdoor.IRC.Zcrew (Aliases: IRC/Flood.bi, Backdoor.IRC.Zcrew): This is a backdoor Trojan that is similar to other backdoor IRC Trojans, such as Backdoor.IRC.Aladinz and Backdoor.IRC.Flood. It is written as an IRC script and uses the mIRC client to connect to the Internet, where it notifies the malicious user of its presence. The malicious user can send various commands to the infected computer and take full control over it. An infected computer can also be used to launch a ping flood attack against another computer at a specified IP address.

Backdoor.Khaos (Aliases: BKDR_KHAOS.A, Backdoor.Khaos, Backdoor.Win32/Khaos): This is a backdoor Trojan that gives a malicious user unauthorized access to your computer. It usually arrives as the file, Server2.exe. By default it opens port 6969 for listening. Backdoor.Khaos does not automatically install itself, as some other program usually installs it. As a result, even if Backdoor.Khaos is installed, in most cases, it will no longer run after you restart your computer. It is written in Microsoft Visual Basic 5 and it requires that the Visual Basic (VB) run-time libraries be installed on your computer in order for it to execute.

Backdoor.Kilo: This is a backdoor Trojan that uses an IRC channel to contact a malicious user. Backdoor.Kilo is written in the Delphi programming language and is packed with UPX. When executed, it copies itself as %System%\Njgal.exe and adds the value, "Boot Manager %System%\Njgal.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Next it opens ports 6711 and 6718 and creates the file, %System%\Boot.dat.

Backdoor.Optix.04.d (Aliases: Backdoor.Optix.04.f, Backdoor-RS): This is a backdoor Trojan and a variant of Backdoor.Optix.04.c. It is a Delphi application packed with UPX, v0.76.1-1.20. By default, it listens on port 5151. Backdoor.Optix.04.d attempts to terminate or close any processes of, or windows belonging to, various programs. These programs include antivirus and security programs.

Backdoor.Optix.05 (Aliases: Backdoor.Optix.50, Backdoor.Win32/Optix.5_0): This is a backdoor Trojan that is a variant of Backdoor.Optix.04.c. By default, it listens on port 5151. The Trojan attempts to terminate or close any processes or windows belonging to various programs, including antivirus and security programs.

Backdoor.SchoolBus.B (Alias: Backdoor.SchoolBus.c): This is a backdoor Trojan that copies files to different locations on your computer and then runs those files. When these files are run they attempt to delete various Windows files and send system information to malicious users.

Backdoor.SilverFTP (Aliases: Backdoor.SilverFTP.10, Backdoor:Win32/SilverFTP.1_0): This is a backdoor Trojan that gives a malicious user unauthorized access to your computer. It copies itself as %Windir%\Wincfg32.exe. When Backdoor.SilverFTP runs, it copies itself as %Windir%\Wincfg32.exe and creates the value, "Windows Config Loader %Windir%\Wincfg32.exe," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start Windows. After the Trojan is installed, it notifies the client side and waits for the commands from the remote client. These commands give a malicious user full access to the file system of the infected computer.

Backdoor.Snowdoor (Aliases: Backdoor.Snowdoor, Backdoor:Win32/Snowdoor.A): This is a backdoor Trojan that opens TCP port 5326 or 5328 on the infected computer. The Trojan allows unauthorized access to an infected computer. It is written in the Delphi programming language and is packed with UPX.

DoS-iFrameNet (Aliases: HTML_CRINET.A, Trojan.VBS.IFrame, VBS/DDoS-iFrameNet): This Trojan exists as a VBScript in an HTML document. It attempts to open hundreds of TELNET sessions by creating an iFrame with the source being a Telnet:// address.

JS/Seeker-C (Aliases: Trojan.JS.Seeker.b, JS/Seeker.gen.a trojan): This is a malicious script. The script attempts to modify Internet Explorer settings, such as the Start Page and Search setting. It appears that the script has been designed to do this to redirect traffic to websites (typically the website redirected to will be pornographic, but there is no reason why it could not be another type of website desiring more business). The Trojan writes to registry values under:

- HKCU\Software\Microsoft\Internet Explorer.

JS/Seeker-C does not forward itself to other users, but has to be deliberately installed on a website or forwarded via e-mail from a malicious user.

Pac (Alias: Trojan.Win32.Pac): This Trojan has been reported in the wild. It is a new P2P (peer-to-peer) worm, backdoor, and DoS (Denial of Service) attack tool. The worm travels from one system to another as an EXE bundle that acts as a dropper. When the dropper is run, it activates the embedded P2P worm. The worm installs itself to system as SYSTEM32.EXE file. It sets a hidden attribute to its file. To start its file during every Windows session, the worm creates the following startup keys for it in the Registry:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "SystemSAS" = "system32.exe"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices "SystemSAS" = "system32.exe"

Being active the worm copies itself to shared folders of popular file sharing clients KaZaA and iMesh. The worm changes the size of its files to make them match (to some extent of course) the size of software packages it tries to fake. Anyone connecting with KaZaA or iMesh client to an infected computer will discover these fake files. If at least one of these files is downloaded and executed by another person, that computer also becomes infected. The worm has backdoor capabilities. It is controlled via a bot that the worm creates in the specific channel on an IRC server. A malicious user can obtain system information, upload, download, execute files on an infected system, and update the worm's file to a newer version. The worm can be used to perform a DoS (Denial of Service) attack. It can perform a SYN flood attack.

PWS-Aileen: This password-stealing Trojan attempts to retrieved cached passwords on the local system and e-mail them to the author. When run, it expects the filename of the Trojan executable to be nudeAileen.scr. If this is the filename, the Trojan copies itself to the %TEMP% directory as dancingBaby.exe. Regardless of the filename, a registry run key is created to load the Trojan at startup (whether it was copied to the %TEMP% directory or not).

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ Run\dancingBaby = %TEMP%\dancingBaby.exe

It tries to create an HTML document, strTempHtm.htm, and load it. This document contains a form with an action that points to a remote mailer script on a trellix.com web page. This results in cached passwords getting mailed to the Trojan author.

Tellafriend.Trojan (Alias: Tellafriend): This Trojan was created by ZeroPopUp. Once installed, it sends an e-mail message to all the contacts in your Windows and Microsoft Outlook address books directing them to download them to download the installer from the host's website. (For the program to be installed, you need to agree to install it by clicking Yes when you see the dialog box shown below.)

Tr/SpBit.A: When executed, Tr/SpBit.A drops numerous files in the C directory. The Trojan installs only .LNK files for http websites. On these websites a user is prompted to download dialer software:

Troj/TKBot-A (Aliases: Backdoor.IRC.Demfire, IRC-Sdbot.dr trojan, Backdoor.Tkbot): This is an IRC backdoor Trojan principally targeted at computers running Microsoft IIS version 4 or 5 on Windows NT/2000 and exploiting the "Web Server Folder Traversal" security vulnerability. A description and patch for this vulnerability can be found at Microsoft Security Bulletin MS00-78. When executed, the Trojan creates the folder \<Program Files>\Microsoft\Update\DLL\tk and copies thirty files into this folder. Two of these files, rundll.exe and mstaskmgr.exe, will be started up as services using the clean application FireDaemon.exe which is also packaged with this Trojan. Rundll.exe is the server component of a commercially available FTP server application. Mstaskmgr.exe is a modified mIRC client that works in conjunction with the mIRC script in the file task.cnf to form the core of the backdoor capabilities of this Trojan. The Trojan listens on a particular IRC channel waiting for a connection from a malicious user. A malicious user who connects to this channel will be able to issue commands to Troj/TKBot-A that will then be interpreted as actions to run on the victim's computer. These commands include being able to upload/download files to and from the victim's machine, remotely running executables and accessing information about the victim's computer. The file vmz.exe, also installed in the main folder, contains a self extracting archive that if executed will create the folder \<Windows>\System32\Microsoft\Crypto into which a further thirteen files are copied. The service svhost is then started from the file scvhost.exe. The file scvhost.exe contains an IRC file server application.

Trojan.ProteBoy (Alias: Trojan.Win32.Proteboy): This is a Trojan Horse that deletes the registry backup files. It is written in Microsoft Visual Basic, version 6, and is packed with UPX. The existence of the file ProtectBoy.com is an indication of a possible infection.

Trojan.Idly: This is a Trojan that attempts to gather system information, including your dial-up networking user name and passwords, and send them to the malicious user. When it is executed, it copies itself as %System%\Msatcl32.exe and adds itself as a reference to Msatcl32.exe to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\RunOnce

Next it creates the file, %System%\IdleUI.exe. The Trojan uses this file, which, by itself, does not contain malicious code. This Trojan also sends information to a variety of Web sites. The Trojan may also be able to download content from these Web sites.

W32.Benpao.Trojan: This is a Trojan horse that steals user password and other information. It also modifies the registry such that opening any .chm, .exe, .ini, .reg, .txt, or .scr file will result in executing the Trojan. It is written in the Visual Basic programming language and is packed with UPX, v0.76.1-1.20.

W32/Igloo-15 (Aliases: Backdoor.Igloo.15.b, Win32/BearBritney.A worm, WORM_GOOL.A, Kazoa.C, W32/Gool.worm, Win32.Igloo.15.trojan, W32/Gool.worm.cfg, Win32.Igloo.00.config): This is a backdoor Trojan and Internet worm which spreads via file sharing on KaZaA networks and via IRC channels. When first run W32/Igloo-15 copies itself to the Windows System folder as Explorer.exe and RealWayToHack.exe and creates the following registry entry so that Explorer.exe is run automatically each time Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\EXPLORER = %System%\EXPLORER.EXE

W32/Igloo-15 runs continuously in the background, listening on a port, allowing a remote user (using a client program) to gain access and control over the computer. The worm creates the folder %Windows%\Sys32 and copies itself to this folder using various filenames. The worm makes the folder %Windows%\sys32 shareable on KaZaA networks by setting the following registry entries:

- HKCU\Software\Kazaa\LocalContent\dir0 = 012345:%Windows%\sys32
- HKCU\Software\Kazaa\LocalContent\dir1 = 012345:%Windows%\sys32
- HKCU\Software\Kazaa\LocalContent\dir2 = 012345:%Windows%\sys32
- HKCU\Software\Kazaa\LocalContent\dir3 = 012345:%Windows%\sys32
- HKCU\Software\Kazaa\LocalContent\dir4 = 012345:%Windows%\sys32
- HKCU\Software\Kazaa\LocalContent\dir5 = 012345:%Windows%\sys32
- HKCU\Software\Kazaa\LocalContent\DisableSharing = 0

It also drops and runs %System%\Explorer.vbs, which infects the mIRC initialization file mirc.ini. Each time a mIRC session is started mirc.ini is loaded automatically and sends the worm to any users who join

any of the current channels. W32/Igloo-15 may terminate selected anti-virus or firewall applications and also sets the following registry entry:

- HKCU\Software\Microsoft\Internet Explorer\Main\RegisteredOrganization = http://www.crash.com

WORM_IXAS.A (Aliases: I-Worm.Ixas, W32/Ixas@MM, W32/GvoWFI.A@mm) (Internet Worm): This nondestructive, non-memory resident worm propagates via e-mail using MAPI (Messaging Application Programming Interface) or SMTP (Simple Mail Transfer Protocol). Upon execution, it drops a copy of itself using a random filename in the Windows system folder. The file name is the base file name of the dropped copy of the worm, i.e. if the dropped copy is ypacww.exe, then the e-mail address will be ypacww@delfi.lt. This worm exploits a known vulnerability affecting unpatched Internet Explorer–based clients, which is commonly known as Automatic Execution of Embedded MIME type. This vulnerability enables e-mail attachments to execute automatically without the recipient opening or double-clicking it. This worm runs on Windows 95, 98, ME, NT, 2000 and XP platforms.

WORM_YAHA.K (Aliases: Win32/Yaha.K, I-Worm.Lentin.i, Win32/Yaha.K@mm, W32/Yaha-K, W32.Yaha.K@mm, W32/Yaha.k): (Internet Worm): This mass-mailing worm uses its own SMTP engine to propagate via e-mail as an attachment, mailing itself to addresses retrieved from the infected system's Windows Address Book (WAB), Yahoo Messenger, MSN and .NET Messenger Services, and files found in all directories with extension names containing the string "HT." It randomly selects the contents of its e-mail subject line, message body, and attachment name from preset information in its code. Because of its very smart stealth and anti-anti-virus technique, most common AV software can't detect or clean it. Like the other YAHA worm variants, this malware also terminates certain processes from memory that are related to popular antivirus and security software. This variant exhibits the following payloads:

- Displays a message box
- Swaps the left and right click mouse functions
- Drops a hidden non-malicious text file in the Windows desktop
- Hides files and folders in the Personal folder (usually C:\My Documents)
- Modifies the Internet Explorer home page.

This worm launches a DoS attack against a particular site and terminates the Task Manager under Windows NT, 2000, and XP. It runs on Windows 9x, NT, 2000, ME, and XP.

W32.Yinker.Trojan (Alias: Trojan.Win32.Yinker: This Trojan creates a new user named Yinker and adds this user to the Administrator group on Windows NT4.0/2000/XP. W32.Yinker.Trojan also stops and restarts the Telnet service.